(e)

ELECTRONIC MONEY

Patent Number: JP9128464
Publication date: 1997-05-16

Inventor(s): HIRASAWA MASANORI
Applicant(s): KOKUSAI GIJUTSU KAIHATSU KK

Requested Patent: JP9128464
Application Number: JP19950286187 19951102
Priority Number(s):
IPC Classification: G06F19/00; G07F7/08; G09C1/00; H04L9/10
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To prevent appropriation of cash information by wiretap of communication by receiving and paying money from/to external equipment by means of a communication means. SOLUTION: The electronic money 10 consists of two LSI chips for communication. LSI-B 12 executes first cipher information communication except for the exchange of cash information and outputs a command for giving instruction for reception or payment of money. On the other hand, LSI-A 11 records cash information and executes second cipher information communication for receiving and paying money from/to the external equipment based on the received command. In the period of this second cipher information communication, LSI-B 12 executes signal passage processing. The two pieces of cipher information makes it difficult to decipher a ciphered code. If the second cipher information communication is made an unopened system in particular, it is extremely difficult to decipher cipher information even though the wire is tapped.

(e)

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－128464

(43)公開日　平成９年(1997)５月16日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	19/00			Ｇ０６Ｆ	15/30	３６０
Ｇ０７Ｆ	7/08		7259－5Ｊ	Ｇ０９Ｃ	1/00	６６０Ｃ
Ｇ０９Ｃ	1/00	６６０		Ｇ０７Ｆ	7/08	Ｊ
Ｈ０４Ｌ	9/10			Ｈ０４Ｌ	9/00	６２１Ｚ

審査請求　未請求　請求項の数11　ＯＬ　（全 18 頁）

(21)出願番号　特願平7－286187

(22)出願日　平成７年(1995)11月２日

(71)出願人　000170554
国際技術開発株式会社
東京都杉並区天沼２丁目３番９号

(72)発明者　平澤　正憲
埼玉県所沢市花園一丁目2423番地の13

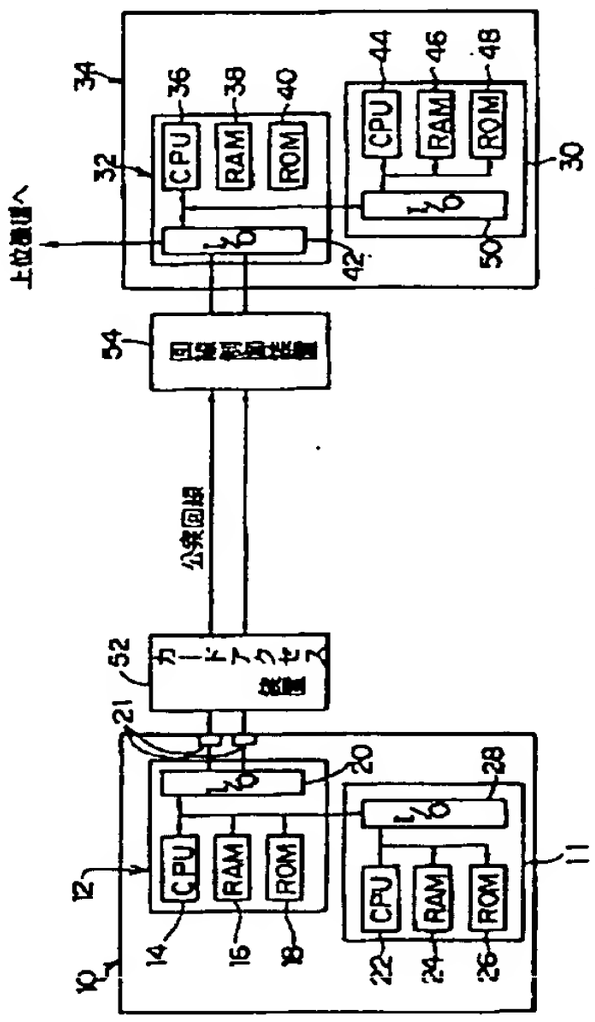
(74)代理人　弁理士　中島　淳　（外２名）

(54)【発明の名称】　電子マネー

(57)【要約】

【課題】　通信手段により外部機器に対して入金、出金等の処理を行い、通信の盗聴による現金情報の盗用を防止する。

【解決手段】　電子マネーを２つの通信用ＬＳＩチップで構成する。ＬＳＩ－Ｂは、現金情報の送受以外の第１の暗号化情報通信を行うと共に、入金や出金を指令するためのコマンドを出力する。一方、ＬＳＩ－Ａは、現金情報を記録すると共に、受信したコマンドに基づいて外部機器に対する入金や出金を行う第２の暗号化情報通信を行う。この第２の暗号化情報通信の間は、ＬＳＩ－Ｂは、信号通過処理を行う。２つの暗号化情報により暗号化コードの解析は困難となる。特に第２の暗号化情報通信を未公開の方式とすれば、通信が盗聴されても暗号化情報の解析はきわめて困難となる。



【特許請求の範囲】
【請求項１】　現金情報に関する暗号化データを外部機器と通信することにより前記外部機器に対する入金又は出金を行う電子マネーであって、
前記外部機器と前記現金情報の送受以外の第１の暗号化情報通信を制御すると共に、前記現金情報の入金又は出金のためのコマンドを出力する第１の通信手段と、
現金情報が記録可能でかつ、前記コマンドを入力した場合には、前記コマンドに基づき前記第１の暗号化情報通信とは異なる第２の暗号化情報通信を前記外部機器と行うことによって前記外部機器に対する入金又は出金を制御する第２の通信手段と、
を有することを特徴とする電子マネー。
【請求項２】　前記第１の通信手段は、前記現金情報の入金又は出金のためのコマンド以外に、少なくとも前記外部機器の有する現金情報の残高チェックのためのコマンド又は前記入金若しくは出金が正常に終了したか否かの状態問い合わせのコマンドを出力すると共に、
前記第２の通信手段は、受信したコマンドに基づいて、前記外部機器との第２の暗号化情報通信を行うことを特徴とする請求項１の電子マネー。
【請求項３】　前記第２の通信手段は、前記外部機器との第２の暗号化情報通信を複数回行うことを特徴とする請求項１又は請求項２の電子マネー。
【請求項４】　前記第２の通信手段は、
前記第２の通信手段により記録されている現金情報の残高を検出すると共に、
前記第２の通信手段により検出された残高が信号として出力される出力端と、
をさらに有することを特徴とする請求項１乃至請求項３のいずれか１項の電子マネー。
【請求項５】　前記第２の通信手段は、
現在の年月日又は時刻を検出する日付手段と、
前記日付手段により検出された年月日又は時刻が、予め設定された有効期限に達した時、前記第２の通信手段への入金を禁止し、少なくとも前記第２の通信手段からの出金を可能とする禁止手段と、
をさらに有することを特徴とする請求項１乃至請求項４のいずれか１項の電子マネー。
【請求項６】　前記第２の通信手段は、
前記コマンドに基づく通信回数を検出する回数検出手段と、
前記回数検出手段により検出された通信回数が予め設定された使用頻度を越えた場合、前記第２の通信手段への入金及び出金を禁止する禁止手段と、
をさらに有することを特徴とする請求項１乃至請求項５のいずれか１項の電子マネー。
【請求項７】　前記第２の通信手段は、
前記現金情報へのアクセスがエラーとなった頻度を検出するエラー頻度検出手段と、
前記エラー頻度検出手段により検出されたエラーの頻度が予め設定されたエラー頻度を越えた場合、前記第２の通信手段からの出金を禁止する禁止手段と、
をさらに有することを特徴とする請求項１乃至請求項６のいずれか１項の電子マネー。
【請求項８】　前記第２の通信手段は、
前記入金又は出金の履歴を記録する履歴手段と、
前記履歴手段により記録された前記入金又は出金の履歴が信号として出力される出力端と、
をさらに有することを特徴とする請求項１乃至請求項７のいずれか１項の電子マネー。
【請求項９】　前記第１の通信手段は、
予め登録されたアクセス先に対してのみ前記入金又は出金を可能とする限定手段と、
をさらに有することを特徴とする請求項１乃至請求項８のいずれか１項の電子マネー。
【請求項１０】　前記第１の通信手段は、
使用者を特定するための暗号コードを有し、入力された番号が前記暗号コードと一致した場合にのみ、前記コマンドによる前記現金情報へのアクセスを可能とする認証手段と、
をさらに有することを特徴とする請求項１乃至請求項９のいずれか１項の電子マネー。
【請求項１１】　前記第２の暗号化情報通信が未公開であることを特徴とする請求項１乃至請求項１０のいずれか１項の電子マネー。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報として記録された現金を有し、該現金に関する暗号化データを外部機器と通信することにより現金情報の入金又は出金を行うＩＣカード等の電子マネーに係り、特に防犯機能のさらなる向上を図った電子マネーに関する。
【０００２】
【従来の技術】従来、預金口座への現金の入金や他の口座への現金の出金等を自動的に行うシステムとして銀行等に設置されている現金自動支払いシステムがある。
【０００３】この現金自動支払いシステムでは、銀行が預金者に発行したプラスティック製の磁気カード、所謂キャッシュカードを介して取引ができるようになっている。この磁気カードには、預金者である使用者の指定口座番号等の所定の情報が磁気的に記録されており、使用者がこのカードを現金自動支払いシステムに挿入し、予めシステムに登録された暗証番号を入力すると、システムは、カードに記録されている口座番号等を読み出し、この口座番号に対応する登録暗証番号と入力された番号とが一致するか否かを判定する。そして、暗証番号が一致した時にのみ、現金の払出し等の処理を行うようになっている。
【０００４】

【発明が解決しようとする課題】しかしながら、上記従来の技術では、預金者が銀行や自動支払いサービスコーナー等に出向かなければ処理することができず、また、磁気カードそのものには現金としての機能がなく、このため銀行が現金を扱う量を減らすことができない、という問題点が生じる。

【０００５】本発明は上記事実を考慮し、情報として記録された現金を有し、通信手段を介して現金の入金、出金等の処理を行うことができると共に、通信の盗聴による現金情報の盗用を防止した電子マネーを提供することが目的である。

【０００６】

【課題を解決するための手段】以上のような課題を解決するため、請求項１の発明は、現金情報に関する暗号化データを外部機器と通信することにより前記外部機器に対する入金又は出金を行う電子マネーにおいて、前記外部機器と前記現金情報の送受以外の第１の暗号化情報通信を制御すると共に、前記現金情報の入金又は出金のためのコマンドを出力する第１の通信手段と、現金情報が記録可能でかつ、前記コマンドを入力した場合には、前記コマンドに基づき前記第１の暗号化情報通信とは異なる第２の暗号化情報通信を前記外部機器と行うことによって前記外部機器に対する入金又は出金を制御する第２の通信手段と、を有することを特徴とする。

【０００７】請求項１の発明では、第１の通信手段が、外部機器と現金情報の送受以外の第１の暗号化情報通信を制御すると共に、現金情報の入金又は出金のためのコマンドを出力する。ここで、入金とは、電子マネーから外部機器への入金をいい、電子マネー側からみた場合、現金情報の出金を意味する。また、出金とは、外部機器から電子マネーへの出金をいい、電子マネー側からみた場合、現金情報の入金を意味する。そして、第２の通信手段は、現金情報が記録可能であると共に、第１の通信手段からのコマンドを入力した場合には、当該コマンドに基づき第１の暗号化情報通信とは異なる第２の暗号化情報通信を外部機器と行うことによって外部機器に対する入金又は出金を制御する。ここで、第１の通信手段及び第２の通信手段を各々ＬＳＩチップで構成することができる。また、第２の暗号化情報通信の間は、第１の通信手段を構成するＬＳＩチップで信号通過処理を行うようにしても良い。

【０００８】以上のように、本発明では、通信によって遠隔にある外部機器との入金、出金の取引が可能となる。また、第１の通信手段による第１の暗号化情報通信と、第２の通信手段による第２の暗号化情報通信という互いに異なる暗号化方式を用い、しかも暗号化方式の切り換え時を外部から判定することが困難であるので、暗号化情報を解析することはきわめて困難となり、防犯効果が向上する。

【０００９】請求項２の発明は、請求項１の前記第１の通信手段が、前記現金情報の入金又は出金のためのコマンド以外に、少なくとも前記外部機器の有する現金情報の残高チェックのためのコマンド又は前記入金若しくは出金が正常に終了したか否かの状態問い合わせのコマンドを出力すると共に、請求項１の前記第２の通信手段が、受信したコマンドに基づいて、前記外部機器との第２の暗号化情報通信を行うことを特徴とする。

【００１０】請求項２の発明では、第１の通信手段が、外部機器の有する現金情報の残高チェックのためのコマンド又は入金若しくは出金が正常に終了したか否かの状態問い合わせのコマンドを出力する。そして、第２の通信手段が入力したコマンドに基づいて外部機器との第２の暗号化情報通信を行う。これにより、入金又は出金以外に、通信によって銀行口座の残高チェックや状態問い合わせが可能となる。

【００１１】請求項３の発明は、請求項１又は請求項２の前記第２の通信手段が、前記外部機器との第２の暗号化情報通信を複数回行うことを特徴とする。

【００１２】請求項３の発明では、第２の通信手段が、外部機器との第２の暗号化情報通信を複数回行う。この複数回のデータ送受によって、暗号化情報の機密性が高まり、防犯効果のさらなる向上が得られる。

【００１３】請求項４の発明は、請求項１乃至請求項３のいずれか１項の前記第２の通信手段が、前記第２の通信手段により記録されている現金情報の残高を検出すると共に、前記第２の通信手段により検出された残高が信号として出力される出力端と、をさらに有することを特徴とする。

【００１４】請求項４の発明では、第２の通信手段が現金情報の残高を検出し、残高の信号を出力端から出力する。この残高の信号を表示すれば、当該電子マネーにおける現金情報の残高を直ちに知ることができる。

【００１５】請求項５の発明は、請求項１乃至請求項４のいずれか１項の前記第２の通信手段が、現在の年月日又は時刻を検出する日付手段と、前記日付手段により検出された年月日又は時刻が、予め設定された有効期限に達した時、前記第２の通信手段への入金を禁止し、少なくとも前記第２の通信手段からの出金を可能とする禁止手段と、をさらに有することを特徴とする。

【００１６】請求項５の発明では、日付手段が現在の年月日又は時刻を検出する。そして、禁止手段は、検出された年月日又は時刻が、予め設定された有効期限に達した時、第２の通信手段への入金を禁止し、少なくとも第２の通信手段からの出金（払出し）を可能とするように制御する。

【００１７】請求項６の発明は、請求項１乃至請求項５のいずれか１項の前記第２の通信手段が、前記コマンドに基づく通信回数を検出する回数検出手段と、前記回数検出手段により検出された通信回数が予め設定された使用頻度を越えた場合、前記第２の通信手段への入金及び

出金を禁止する禁止手段と、をさらに有することを特徴とする。
【００１８】請求項６の発明では、回数検出手段がコマンドに基づく前記第２の通信手段の通信回数を検出する。そして、禁止手段は検出された通信回数が予め設定された使用頻度を越えた場合、第２の通信手段への入金及び出金を禁止するように制御する。
【００１９】請求項７の発明は、請求項１乃至請求項６のいずれか１項の前記第２の通信手段が、前記現金情報へのアクセスがエラーとなった頻度を検出するエラー頻度検出手段と、前記エラー頻度検出手段により検出されたエラーの頻度が予め設定されたエラー頻度を越えた場合、前記第２の通信手段からの出金を禁止する禁止手段と、をさらに有することを特徴とする。
【００２０】請求項７の発明では、エラー頻度検出手段が現金情報へのアクセスがエラーとなった頻度を検出し、禁止手段は、検出されたエラーの頻度が予め設定されたエラー頻度を越えた場合、第２の通信手段からの出金を禁止するように制御する。
【００２１】請求項５～請求項７の発明により、防犯効果がさらに向上する。請求項８の発明は、請求項１乃至請求項７のいずれか１項の前記第２の通信手段が、前記入金又は出金の履歴を記録する履歴手段と、前記履歴手段により記録された前記入金又は出金の履歴が信号として出力される出力端と、をさらに有することを特徴とする。
【００２２】請求項８の発明では、履歴手段が入金又は出金の履歴を記録し、出力端から記録された履歴信号を出力する。これによって、外部機器と離れた箇所でも入金及び出金の履歴を直ちに知ることができる。
【００２３】請求項９の発明は、請求項１乃至請求項８のいずれか１項の前記第１の通信手段が、予め登録されたアクセス先に対してのみ出金を可能とする限定手段と、をさらに有することを特徴とする。
【００２４】請求項９の発明は、請求項１乃至請求項８のいずれか１項の前記第１の通信手段が、予め登録されたアクセス先に対してのみ前記入金又は出金を可能とする限定手段と、をさらに有することを特徴とする。
【００２５】請求項９の発明では、限定手段は、予め登録されたアクセス先に対してのみ入金又は出金を可能とするように制御する。
【００２６】請求項１０の発明は、請求項１乃至請求項９のいずれか１項の前記第１の通信手段が、使用者を特定するための暗号コードを有し、入力された番号が前記暗号コードと一致した場合にのみ、前記コマンドによる前記現金へのアクセスを可能とする認証手段と、をさらに有することを特徴とする。
【００２７】請求項１０の発明では、電子マネーは使用者を特定するための暗号コードを有しており、認証手段が入力された番号が暗号コードと一致した場合にのみ、前記コマンドによる前記現金へのアクセスを可能とするように制御する。
【００２８】このように電子マネー自体に認証機能を付加することにより、防犯効果はさらに向上する。
【００２９】請求項１１の発明は、請求項１乃至請求項１０のいずれか１項の前記第２の暗号化情報通信が未公開であることを特徴とする。
【００３０】請求項１１の発明では、未公開の第２の暗号化情報通信が行われる。これにより、暗号化データの解析はさらに困難となり、さらに防犯効果を向上させることができる。
【００３１】
【発明の実施の形態】本発明の実施の形態を図１乃至図１６にしたがって説明する。
【００３２】図１に、本発明の実施の形態に係る電子マネー１０と外部機器３４の構成、及びこれらの機器が公衆回線によって接続されている状態を示す。なお、外部機器３４として、例えば現金自動支払いシステムや自動販売機等がある。
【００３３】図１に示すように、本実施の形態に係る電子マネー１０は、ＬＳＩチップ１１（以下、ＬＳＩ－Ａという）及びＬＳＩチップ１２（以下、ＬＳＩ－Ｂという）を含んだ所謂ＩＣカードとして構成されている。ここで、ＬＳＩ－Ａは、情報としての現金（現金情報）を記録すると共に、現金情報の出し入れを管理・制御するための電子財布としての機能を有する。このＬＳＩ－Ａは、ＬＳＩチップ全体の管理・制御を実行するＣＰＵ２２と、現金情報を記録するためのＲＡＭ２４と、ＲＯＭ２６と、Ｉ／Ｏポート２８と、から構成されており、各々がデータやコマンドを伝達するためのバスによって接続されている。なお、電子マネー１０に電源が内蔵されていない場合には、電源の供給がオフになったとしても記録された現金情報が失われないようにＲＡＭ２４として、データのリード／ライトが可能な不揮発性メモリが用いられる。
【００３４】また、ＲＯＭ２６には、制御用のプログラムが格納されており、ＣＰＵ２２は、このプログラムに基づいて、ＬＳＩ－Ｂから出力されてきたコマンドを解析し、該コマンドに基づいて外部機器３４との通信制御を実行し、ＲＡＭ２４に記録された現金情報の入金や出金等の制御を行う。
【００３５】また、図１６に示すように、ＬＳＩ－Ａの Ｉ／Ｏポート２８には、年月日又は時刻をカウントするクロック２７が接続されており、ＣＰＵ２２は、クロック２７によりカウントされた年月日又は時刻を検知できるようになっている。
【００３６】また、Ｉ／Ｏポート２８には、光を検出する光センサー２９が接続されており、光センサー２９が光を検出すると、検出信号をＣＰＵ２２に伝達する。なお、光センサー２９は、ＬＳＩ－Ａのケーシングの外部

に配置されている。さらに、Ｉ／Ｏポート２８には、予備電源１３が接続されており、本来の電源が供給されていない場合でも、光センサー２９が光を検出した場合には、ＣＰＵ２２やＲＡＭ２４等へ電源が供給されるようになっている。

【００３７】一方、ＬＳＩ－Ｂは、外部機器３４との通信のインターフェイス制御を行うと共に、ＬＳＩ－Ａを制御するための複数種類のコマンドを出力する。このインターフェイス制御では、外部機器３４の種類に応じて通信を制御するようになっている。

【００３８】図１に示すように、ＬＳＩ－Ｂは、ＬＳＩチップ全体の管理・制御を実行するＣＰＵ１４と、外部機器３４から送られてきたデータが記憶されるＲＡＭ１６と、ＲＯＭ１８と、Ｉ／Ｏポート２０と、から構成されており、各々がデータやコマンドを伝達するためのバスによって接続されている。また、このバスには、ＬＳＩ－ＡのＩ／Ｏポート２８が接続されている。

【００３９】また、Ｉ／Ｏポート２０には、図示しない電源、後述するカードアクセス装置５２及び外部機器３４との信号の受け取り受渡しを行うための電気接点２１が接続されている。

【００４０】また、ＲＯＭ１８には、制御用のプログラムが格納されており、ＣＰＵ１４は、このプログラムに基づいて外部機器３４との通信制御を実行し、外部機器３４から送られてきた暗号化データを解読し、解読されたデータに基づいて、入金や出金等を行うためのコマンドをＬＳＩ－Ａに出力する。

【００４１】また、電子マネー１０は、公衆回線にアクセスして外部機器３４と接続するためのカードアクセス装置５２を介して外部機器３４と通信を行うようになっている。このカードアクセス装置５２の詳細な構成を図２に示す。図２に示すように、カードアクセス装置５２は相手先との通信に必要な情報や電子マネー１０への指令等を入力するためのキーボード６６及び電気接点２１から出力された入金、出金の履歴、電子財布等の残高情報を表示するディスプレー６８を備え、内部には電子マネー１０を内部へ搬送する搬送装置７０が設けられている。搬送装置７０は、所定の間隔に配設された挟持ローラー対７２、７４を備え電子マネー１０を挟持して、図２の矢印Ａ方向及び矢印Ａ方向とは反対方向に搬送する。

【００４２】挟持ローラー対７２と挟持ローラー対７４の間には、電子マネー１０の電気接点２１に接触する接触端子７６が設けられている。

【００４３】この接触端子７６はＩ／Ｏポート６４を介して公衆回線との接続を制御する回線制御装置６０及びモデム６２に接続されている。さらに接触端子７６には、カードアクセス装置５２の図示しない電源が接続されており、該電源の供給によって電子マネー１０が動作するようになっている。

【００４４】一方、外部機器３４は、公衆回線の接続の制御を行う回線制御装置５４を介して電子マネー１０と接続されている。

【００４５】外部機器３４は、電子マネー３４と同様にＬＳＩチップ３０（以下、ＬＳＩ－Ａ'という）及びＬＳＩチップ３２（以下、ＬＳＩ－Ｂ'という）の２つのＬＳＩチップを含んで構成されている。

【００４６】ここで、外部機器３４が現金自動支払いシステムの場合、ＬＳＩ－Ａ'は、ＲＡＭ４６に口座毎に記録された現金情報（電子預金）の出し入れを管理する機能を有する。なお、ＲＡＭ４６として、電子マネー１０のＲＡＭ２４と同様に、不揮発性メモリを使用しても良い。

【００４７】また、ＬＳＩ－Ｂ'のＩ／Ｏポート４２には、ホストコンピュータ等の上位機種が接続されており、口座に関する情報等をやり取りできるようになっている。なお、上記以外のＬＳＩ－Ａ'及びＬＳＩ－Ｂ'の構成及び機能は、各々電子マネー１０のＬＳＩ－Ａ及びＬＳＩ－Ｂとほぼ同様であり、詳細な説明を省略する。

【００４８】次に、電子マネー１０と外部機器３４との通信処理の概要を図３によって説明する。

【００４９】図３に示すように、まずＬＳＩ－ＢとＬＳＩ－Ｂ'との間で所定の手順に従って第１の暗号化情報通信を行う（ステップ９０）。この通信では、電子マネー１０が外部機器３４と現金情報に関する取引を行う上で必要となる情報が、相手先の外部機器３４に送信される。

【００５０】ところで、ＬＳＩ－ＢとＬＳＩ－Ｂ'との間の通信では、防犯効果を高めるために送信するコードにスクランブルをかけて暗号化している。

【００５１】次に、この暗号化方法について説明する。例えば送信するコードの列が例えば６４ビットであるとする。

【００５２】６４ビットのコードは、所定の方法で例えば８ビット×８列のマトリックスに変更され、各行、各列が所定の方法にしたがってそれぞれローテートされる。ローテートされたマトリックス状のコードは再び所定の方法で６４ビット列にされ、暗号化が完了する。

【００５３】本実施の形態では、８ビット×８列のマトリックスにされたコードの各行、各列のローテートの回数及び８ビット×８列のマトリックスにされたコードを６４ビット一列にする方法のそれぞれを変えることによって、複数個の暗号化方法を得ている。

【００５４】なお、暗号化の方法を選択するにあたっては、それぞれの暗号化の方法に番号を付し、暗号化の方法の番号に応じた乱数を発生させるようにすればよい。例えば、暗号化の方法が１００通りあったとすると、各暗号化の方法に１～１００までの番号を付して暗号化方法と共に暗号化テーブル（図１５参照）としてＲＯＭ１

８に記憶しておく。
【００５５】さらにＬＳＩ－Ｂ及びＬＳＩ－Ｂ’では、ＣＰＵ１４及びＣＰＵ３６によりシードデータに基づいて乱数が生成されるようになっており、乱数を暗号化の方法の番号に対応させて１～１００までの何れか１つを生成するようにする。暗号化するに当たっては、その時に生成された乱数に対応した暗号化方法にしたがって送信するコードを暗号化する。なお、暗号化されたデータには、所定の位置に、暗号化の方法を示す暗号化コードを付け加える。
【００５６】一方、復号側にも、暗号側と同様の暗号化テーブルが記憶されており、復号は、暗号化コードに基づいて暗号化の逆の手順で行う。即ち、６４ビットの暗号化されたコードが、暗号化と逆の手順にしたがって８ビット×８列のマトリックスに戻され、各行、各列がそれぞれ上記と逆にローテートされ、再び６４ビット一列にされて元のコードが得られる。
【００５７】図３のステップ９０の通信が終了すると、外部機器３４においてＬＳＩ－ＢからＬＳＩ－Ｂ’に送出された情報が正しい情報であるか否かが判定される（ステップ９２）。情報が正しいと判定された場合（ステップ９２肯定判定）にのみ次のステップ９４に進み、情報に誤りがある場合（ステップ９２否定判定）には、通信処理を終了する。
【００５８】ステップ９４では、ＬＳＩ－Ｂ及びＬＳＩ－Ｂ’が現金情報の出し入れ等を制御するためのコマンドを生成し、各々ＬＳＩ－Ａ及びＬＳＩ－Ａ’に出力する（ステップ９４）。なお、ＬＳＩ－ＢとＬＳＩ－Ａの間の通信、ＬＳＩ－ＢとＬＳＩ－Ａの間の通信では、暗号化情報を用いない通常の通信を用いても良い。
【００５９】次に、ＬＳＩ－Ｂ及びＬＳＩ－Ｂ’が各々信号通過処理を行う（ステップ９６）。すなわち、ＬＳＩ－Ｂ、Ｂ’が各々のバスをＬＳＩ－Ａ、Ａ’に開放すると共に、通信制御を一時的に停止する。この処理によって、ＬＳＩ－Ａ、ＬＳＩ－Ａ’との間で異なる通信手順に従った独自の通信が可能となる。
【００６０】次に、ＬＳＩ－ＡとＬＳＩ－Ａ’との間で伝送されたコマンドに基付き現金情報等のコードを暗号化して第２の暗号化情報通信を行う（ステップ９８）。この第２の暗号化情報通信では、ＬＳＩ－Ｂ、Ｂ’間の第１の暗号化情報通信とは異なる暗号化方式が用いられる。本実施の形態では、複数回の通信に分割して第２の暗号化情報通信を行うことにより、暗号化の強度を高めている。ここで、コードを暗号化する方法としては、周知の方法を適用することができるが、特に非公開の暗号化方式を用いる方が防犯効果の点で好ましい。
【００６１】以上のように、ＬＳＩ－Ｂ、Ｂ’間の第１の情報化通信と、ＬＳＩＡ、Ａ’間の第２の情報化通信という互いに異なる暗号化方式を用い、しかも暗号化方式の切り換え時を外部から判定することが困難であるので、暗号コードを解析することはきわめて困難となる。
【００６２】次に、ＬＳＩ－Ａ、Ａ’、ＬＳＩ－Ｂ、Ｂ’の各々の処理の流れについて図４乃至図７のフローチャートによって詳細に説明する。なお、以下の説明では、外部機器３４が現金自動支払いシステムの場合を扱う。
【００６３】まず、ＬＳＩ－Ｂの処理について図４によって説明する。図４に示すように、ＬＳＩ－Ｂへの入力を待機し（ステップ１００否定判定）、入力があった場合（ステップ１００肯定判定）、入力信号がフラグリセット信号以外の信号であるか否かを判定する（ステップ１０２）。
【００６４】入力信号がフラグリセット信号以外の信号である場合（ステップ１０２肯定判定）、フラグF_1が０であるか否かを判定し（ステップ１０４）、フラグF_1が０の場合に（ステップ１０４肯定判定）、入力信号の情報をＲＡＭ１６に記憶する（ステップ１０６）。
【００６５】次に、ＲＡＭ１６に記憶された情報を読み出し、暗号化コードに変換する（ステップ１０８）。そして、前述した第１の暗号化情報通信を外部機器３４のＬＳＩ－Ｂ’と実行する（ステップ１１０）。この通信によって、例えば電子マネー１０にキーボード６６を介して入力された口座番号、当該口座の暗唱番号、及びＩＤコードが相手先の外部機器３４（現金自動支払いシステム）に送信される。また、この暗号化情報通信では、入金、出金、残高チェック等の旨が送信される。なお、ＩＤコードは、当該電子マネー１０を特定するためのコード番号であり、図１４に示すように、通常では書き込み等のアクセスが禁止されているメモリ領域に予め登録されているものである。
【００６６】次に、ＬＳＩ－Ｂ’からの許可信号の受信を待機し（ステップ１１２否定判定）、許可信号を受信した場合（ステップ１１２肯定判定）、ＬＳＩ－Ａへコマンドを出力する（ステップ１１４）。このコマンドは、ステップ１００で入力された情報に基づいて決定され、例えば次のような４種類の機能①～④を各々有するコマンドのいずれか１つが出力される。
【００６７】①　電子預金から電子マネーへの入金（入金コマンド）
②　電子預金から電子マネーへの出金（出金コマンド）
③　電子預金の残高チェック（残高チェックコマンド）
④　通信の状態（入金等が正常に終了したか、アラームが発生したか否か、電子預金の残高が足らなかったか否かの状態）の問い合わせ（状態問い合わせコマンド）
なお、①～④の機能を有するコマンドは、図１３に示すように各々が特定の命令コードによって表される。
【００６８】次に、フラグF_1に１を代入し、再びステップ１００で入力信号を待機する（ステップ１１６）。
【００６９】一方、フラグF_1が０でなかった場合（ステップ１０４否定判定）、前述した信号通過処理を実行

し（ステップ１１８）、再びステップ１００で入力信号を待機する。

【００７０】また、フラグリセット信号が入力された場合（ステップ１０２否定判定）、ステップ１１８の信号通過処理を解除し（ステップ１２０）、フラグF_1に０を代入し（ステップ１２２）、ステップ１００で入力信号を待機する。

【００７１】次に、ＬＳＩ－Ｂ'の処理について図５によって説明する。図５に示すように、ＬＳＩ－Ｂ'への入力を待機し（ステップ１３０否定判定）、入力があった場合（ステップ１３０肯定判定）、入力信号がフラグリセット信号以外の信号であるか否かを判定する（ステップ１３２）。

【００７２】入力信号がフラグリセット信号以外の信号である場合（ステップ１３２肯定判定）、フラグF_2が０であるか否かを判定し（ステップ１３４）、フラグF_2が０の場合には（ステップ１３４肯定判定）、入力信号の暗号化コードを復号化する（ステップ１３６）。

【００７３】次に、復号化された情報が正しいか否かを判定する（ステップ１３８）。例えば、復号化情報から電子預金の口座番号と、暗証番号を読み出し、予めＲＯＭ４０に登録されている当該口座の暗証番号が受信された暗証番号と一致した場合、に情報が正しいと判定する。

【００７４】復号化情報が正しくないと判定した場合（ステップ１３８否定判定）、再びステップ１３０に戻り、入力信号を待機する。一方、復号化情報が正しいと判定した場合には（ステップ１３８肯定判定）、ＬＳＩ－Ｂへ許可信号を送出し（ステップ１４０）、ＬＳＩ－Ａ'へコマンドを出力する。このコマンドは、ＬＳＩ－Ｂから送られてきた暗号化情報に記録されている入金、出金等の別に基づいて、各々に対応する処理をＬＳＩ－Ａ'に実行させるためのものである。すなわち、当該コマンドは、図４のステップ１１４でＬＳＩ－ＡからＬＳＩ－Ａ'へ出力されたコマンドに各々対応する。

【００７５】次に、フラグF_2に１を代入し、再びステップ１３０で入力信号を待機する（ステップ１１６）。

【００７６】一方、フラグF_2が０でなかった場合（ステップ１３４否定判定）、前述した信号通過処理を実行し（ステップ１４６）、再びステップ１３０で入力信号を待機する。

【００７７】また、フラグリセット信号が入力された場合（ステップ１３２否定判定）、ステップ１４６の信号通過処理を解除し（ステップ１４８）、フラグF_2に０を代入し（ステップ１５０）、ステップ１３０で入力信号を待機する。

【００７８】次に、ＬＳＩ－Ａの処理について図６のフローチャートによって説明する。図６に示すように、まず、ＬＳＩ－ＢからＬＳＩ－Ａへのコマンド入力を待機する（ステップ１６０否定判定）。コマンドが入力された場合（ステップ１６０肯定判定）、入力コマンドを判別する（ステップ１６２）。

【００７９】コマンドが入金コマンド又は出金コマンドである場合（ステップ１６４肯定判定）、入金予定額M_{in}又は出金予定額M_{out}を読み出す（ステップ１６６）。図１３に示すように、入金コマンド及び出金コマンドの場合には、各々のコマンドコードに入金予定額M_{in}、出金予定額M_{out}のコードが付加されており、ステップ１６６では、このコードを読み出す処理を行う。入金コマンド及び出金コマンド以外のコマンドの場合（ステップ１６４否定判定）には、当該処理を行わない。

【００８０】次に、ＬＳＩ－Ａ'との第２の暗号化通信を実行する（ステップ１６８）。この通信では、コマンド毎に次のような情報のやり取りが行われる。なお、受信された暗号化コードは予め記憶された復号化方式に従い復号化される。

【００８１】

① 入金コマンド　：　入金予定額M_{in}の送信
② 出金コマンド　：　出金予定額M_{out}の送信
③ 残高チェックコマンド　：　電子預金口座の残高ｍの受信
④ 状態問い合わせコマンド　：　状態情報の受信

ことによって行われる。

ここで、前述したように第２の暗号化情報通信では、暗号化コードを複数回に分割して通信を行っているので、公衆回線への侵入者がM_{in}やM_{out}等の金額を盗聴することはきわめて困難となる。

【００８２】第２の暗号化通信が終了すると（ステップ１７０で肯定判定）、コマンド別に各々の処理を実行する。

【００８３】入金コマンドの場合（ステップ１７２肯定判定）、通信が正常に終了したか否か、すなわちＬＳＩ－Ａ'に入金予定額M_{in}が正常に伝達されたか否かを判定する（ステップ１７４）。この判定は、ＬＳＩ－Ａ'から送られてきた入金正常終了のフラグ信号を解析することによって行われる。

【００８４】通信が正常に終了した場合（ステップ１７４肯定判定）は電子預金への入金が完了した場合であるので、ＬＳＩ－Ａの電子財布に記録されている残高Ｍから入金額M_{in}を引いた値を残高Ｍとする（ステップ１７６）。

【００８５】また、出金コマンドの場合（ステップ１７８肯定判定）、通信が正常に終了したか否かを判定し（ステップ１８０）、通信が正常に終了した場合には（ステップ１８０肯定判定）、さらに電子預金の口座にM_{out}以上の残金があったか否かをＬＳＩ－Ａ'からの受信信号を解析することにより判定する（ステップ１８

２）。
【００８６】電子預金の口座にM_{out}以上の残金がある場合（ステップ１８２肯定判定）、ＬＳＩ－Ａの電子財布に記録されている残高Ｍから電子預金からの出金額M_{out}を加算した値を残高Ｍとする（ステップ１８４）。通信が正常に終了しなかった場合（ステップ１８０否定判定）又は口座にM_{out}以上の残金が無かった場合（ステップ１８２否定判定）には、残高ＭへのM_{out}の加算を行わない。
【００８７】また、残高チェックコマンド又は状態問い合わせコマンドの場合（ステップ１７８否定判定）、ＬＳＩ－Ａからの受信データに記録されている残高ｍ又は状態情報の読み出し、記憶を行う（ステップ１８６）。
【００８８】各コマンド別の処理が終了すると、入出金の履歴がＲＡＭ２４に記録される（ステップ１８８）。なお、この履歴記録では、ＬＳＩ－Ａ側の処理を履歴として記録する方法の他に、電子預金のＬＳＩ－Ａ’から送られてきた当該口座における入出金の履歴を記録するようにしても良い。
【００８９】次に、ＬＳＩ－Ｂの信号通過処理を解除させるためのフラグリセット信号を出力し（ステップ１９０）、再びステップ１６０に戻りコマンド入力を待機する。
【００９０】なお、電子マネー１０では、キーボード６６からの指令信号に基づいて、ステップ１８６で記憶された残高ｍや状態情報、又はステップ１８８で記録された入出金履歴の信号を電気接点２１を介して出力する。出力された残高ｍや状態情報の信号は、ディスプレー６８上に表示され、オペレータは直ちにこれらの情報を知ることができる。
【００９１】次に、ＬＳＩ－Ａ’の処理について図７のフローチャートによって説明する。図７に示すように、まず、ＬＳＩ－Ｂ’からＬＳＩ－Ａ’へのコマンド入力を待機する（ステップ２００否定判定）。コマンドが入力された場合（ステップ２００肯定判定）、入力コマンドを判別する（ステップ２０２）。
【００９２】入力コマンドが残高チェックコマンドの場合（ステップ２０４肯定判定）、電子預金として記録されている指定口座の残高ｍを検出する（ステップ２０６）。また、入力コマンドが状態問い合わせコマンドの場合（ステップ２０８肯定判定）、先の現金情報の通信時にＣＰＵ４４によってＲＡＭ４６に記録された状態情報を読み出す（ステップ２１０）。入金コマンド及び出金コマンドの場合（ステップ２０４否定判定及びステップ２０８否定判定）には、当該処理を行わない。
【００９３】次に、ＬＳＩ－Ａとの第２の暗号化通信を実行する（ステップ２１２）。この通信は、図６のステップ１６８の通信に対応するもので、送受信されるデータが互いに逆の関係になっている。なお、受信された暗号化コードは予め記憶された復号化方式に従い復号化される。
【００９４】第２の暗号化通信が終了すると（ステップ２１２肯定判定）、コマンド別に各々の処理を実行する。
【００９５】入金コマンドの場合（ステップ２１６肯定判定）、通信が正常に終了したか否か、すなわちＬＳＩ－Ａ’に入金予定額M_{in}が正常に伝達されたか否かを判定する（ステップ１７４）。
【００９６】通信が正常に終了した場合（ステップ２１６肯定判定）は、ＬＳＩ－Ａ’の電子財布に記録されている残高ｍに入金額M_{in}を加算した値を残高ｍとする（ステップ２２０）。
【００９７】また、出金コマンドの場合（ステップ２２２肯定判定）、通信が正常に終了したか否かを判定し（ステップ２２４）、通信が正常に終了した場合には（ステップ２２４肯定判定）、さらに残高ｍがM_{out}以上であるか否かを判定する（ステップ２２６）。
【００９８】電子預金の口座にM_{out}以上の残金がある場合（ステップ２２６肯定判定）、残高ｍから出金額M_{out}を引いた値を電子預金の残高ｍとする（ステップ２２８）。通信が正常に終了しなかった場合（ステップ２２４否定判定）又は口座にM_{out}以上の残金が無かった場合（ステップ２２６否定判定）には、当該口座からのM_{out}の出金を行わない。
【００９９】また、状態問い合わせコマンドの場合（ステップ２２２否定判定）、ステップ２１２の第２の暗号化情報通信の通信履歴等に基づいて状態を検出し（ステップ２３１）、検出された状態情報を記憶する（ステップ２３２）。このＬＳＩ－Ａからの受信データに記録されている残高ｍ又は状態情報の読み出し、記憶を行う（ステップ１８６）。
【０１００】各コマンド別の処理が終了すると、ＬＳＩ－Ｂ’の信号通過処理を解除させるためのフラグリセット信号を出力し（ステップ２３４）、再びステップ２００に戻りコマンド入力を待機する。
【０１０１】以上のように、電子マネー１０は２つのＬＳＩチップを有し、各々異なる暗号化方式を用いることによって侵入者を排除しているが、さらに防犯効果を高めるために、以下に述べるような複数の防犯処理が用意されている。これらの処理について図８乃至図１２、及び図１７のフローチャートにより説明する。
【０１０２】まず、有効期限設定処理を図８によって説明する。図８に示すように、電子マネー１０を使用できる有効期限を設定する（ステップ２４０）。この設定では、例えばキーボード６６によって有効期限を入力できるようにし、一度設定された有効期限を変更不可にする。登録された有効期限は、図１４に示すように、メモリ領域の所定箇所に登録される。また、有効期限を入力不可とし、電子マネー１０を使用した時点から予め登録された有効期限を設定するようにしても良い。

【０１０３】次に、年月日又は時刻を検出する（ステップ２４２）。この年月日等のカウントは、例えば図１６のＬＳＩ－Ａの１／Ｏポート２８に接続されたクロック２７が行い、ＣＰＵ２２がそのカウント値を検知できるようになっている。

【０１０４】次に、ステップ２４２で測定された年月日又は時刻が、ステップ２４０で設定された有効期限に達したか否かをＣＰＵ２２が判定する（ステップ２４４）。有効期限に達していない場合には（ステップ２４４否定判定）、再びステップ２４２に戻り、年月日又は時刻の測定を行う。

【０１０５】有効期限に達した場合（ステップ２４４肯定判定）、電子マネー１０への入金を禁止し、電子マネー１０からの払出しのみを可能とする（ステップ２４６）。なお、ステップ２４６の電子マネーへの入金の禁止は、図１４に示すように、メモリ領域に記録されている禁止フラグ（０／１）の値に基づいて行われる。すなわち、ＬＳＩ－Ａは電子財布のＲＡＭ２４へアクセスする場合、入金の禁止フラグ及び払出しの禁止フラグを参照し、禁止フラグが０の場合、電子財布への入金処理を可能とし、禁止フラグが１の場合には、電子財布への入金処理を禁止する。ステップ２４６の場合、入金の禁止フラグが１で、払出しの禁止フラグが０となるようにメモリ領域がアクセスされる。

【０１０６】以上のように電子マネー１０の使用できる有効期限を設定できるようにしたので、電子マネー１０を盗用された場合でも、被害を少なくすることができる。

【０１０７】次に、不正アクセス禁止処理を図９によって説明する。図９に示すように、まず、ＬＳＩ－ＡのＣＰＵ２２がエラー回数Ｅに０を代入する（ステップ２４８）。次に、電子財布への入金、出金等のアクセスを待機する（ステップ２５０否定判定）。

【０１０８】電子財布へのアクセスがあった場合（ステップ２５０肯定判定）、当該アクセスがエラー終了したか否かを判定する（ステップ２５２）。アクセスが正常終了した場合（ステップ２５２否定判定）、ステップ２４８に戻ってエラー回数に０を代入する。一方、電子財布へのアクセスがエラー終了した場合（ステップ２５２肯定判定）、Ｅを１インクリメントし（ステップ２５４）、Ｅが連続エラー回数のしきい値Ｔｈ１を越えたか否かを判定する（ステップ２５６）。なお、連続エラー回数のしきい値Ｔｈ１は、図１４の示すように、メモリ領域の所定箇所に記録されている。Ｅがしきい値Ｔｈ１を越えていない場合（ステップ２５６否定判定）、再びステップ２５０に戻り、電子財布へのアクセスを待機する。

【０１０９】Ｅがしきい値Ｔｈ１を越えた場合（ステップ２５６肯定判定）、電子財布からの払出しを禁止する（ステップ２５８）。なお、この処理の場合には、図１４の払出し禁止フラグが１に、入金フラグが０に設定される。

【０１１０】以上のように連続してＴｈ１を越えたエラー回数が生じた場合には、電子マネー１０の盗用者が電子マネーへのアクセス方法を調べている場合であるとみなし、ＬＳＩ－Ａが電子財布からの払出しを禁止することによって盗用の被害を未然に防止することができる。なお、ステップ２５８で電子財布からの払出しのみを禁止するようにしたが、電子財布への入金も禁止するようにしても良い。

【０１１１】次に、使用頻度制限処理を図１０によって説明する。図１０に示すように、まずＬＳＩ－ＡのＣＰＵ２２が、時間ｔに０を代入し（ステップ２６０）、使用頻度Ｕに０を代入する（ステップ２６２）。

【０１１２】次に、時間をカウントするため、ｔを１インクリメントし（ステップ２６４）、ｔが使用頻度の検出期間のしきい値Ｔｈ２を越えたか否かを判定する（ステップ２６６）。ｔがしきい値Ｔｈ２を越えた場合（ステップ２６６肯定判定）、再びステップ２６０、２６２に戻り、ｔ及びＵを０クリアーして同様の処理を繰り返す。

【０１１３】ｔがしきい値Ｔｈ２を越えていない場合（ステップ２６６肯定判定）、電子財布へのアクセスがあったか否かを判定する（ステップ２６８）。電子財布へのアクセスが無かった場合（ステップ２６８否定判定）、ステップ２６４に戻り、時間ｔをカウントする。

【０１１４】電子財布へのアクセスが有った場合（ステップ２６８肯定判定）、Ｕを１インクリメントし（ステップ２７０）、Ｕが使用頻度のしきい値Ｔｈ３を越えているか否かを判定する（ステップ２７２）。Ｕがしきい値Ｔｈ３を越えていない場合（ステップ２７２否定判定）、ステップ２６４に戻り、時間ｔをカウントする。

【０１１５】Ｕがしきい値Ｔｈ３を越えている場合には（ステップ２７２肯定判定）、デンシ財布へのアクセスを禁止する（ステップ２７４）。すなわち、電子サイフへの入金及び払出しの禁止フラグを１にする。

【０１１６】以上のように、エラー回数だけではなく、正常終了した場合のアクセス回数を含めた使用頻度が大きい場合に入金や払出しを禁止することによって、さらに徹底して盗用による被害を防止することができる。

【０１１７】次に、アクセス可能先設定処理を図１１によって説明する。図１１に示すように、まず、ＬＳＩ－Ｂが相手先と暗号化情報通信を行い（ステップ２８０）、当該通信相手のＩＤ番号を受信する（ステップ２８２）。

【０１１８】次に、ＬＳＩ－ＢのＣＰＵ１４が、予め登録されたアクセス可能先のＩＤ番号の読み出しを行う（ステップ２８４）。なお、アクセス可能先のＩＤ番号は、図１４に示すようにメモリ領域に予め登録されている。そして、通信相手がアクセス可能先であるか否かを

判定する（ステップ２８６）。すなわち、通信相手のＩＤ番号がアクセス可能先のＩＤ番号の中にあるか否かを判定する。

【０１１９】通信相手がアクセス可能先でなかった場合（ステップ２８６否定判定）、ＬＳＩ－Ａへコマンドを出力せず、入金、出金、及び残高チェック等の禁止処理を行う（ステップ２９０）。すなわち、入金、出金等の禁止フラグを１に設定する。なお、残高チェックに関しては図示しないが、入金、出金の禁止フラグと同様に禁止フラグを設けることができる。　一方、通信相手がアクセス可能先である場合には（ステップ２８６肯定判定）、通常通り、入金、出金、及び残高チェック等の処理を実行する（ステップ２８８）。

【０１２０】次に、認証機能を図１２によって説明する。図１２に示すように、キーボード６６を介して暗号コードをＬＳＩ－Ｂに入力する（ステップ３００）。次に、メモリ領域に予め登録されている暗号コードの読み出しを行う（ステップ３０２）。

【０１２１】次に、ＬＳＩ－ＢのＣＰＵ１４が入力された暗号コードと登録されている暗号コードとが一致するか否かを判定する（ステップ３０４）。暗号コードが一致していなかった場合（ステップ３０４否定判定）、ＬＳＩ－Ａへコマンドを出力せず電子財布の入金、出金等の処理を禁止する（ステップ３０６）。

【０１２２】一方、暗号コードが互いに一致した場合には（ステップ３０４肯定判定）、この電子マネー１０を特定するＩＤコードをメモリ領域から読み出し（ステップ３０８）、該ＩＤコードに基づいて相手先と入金、出金等の処理を行う（ステップ３１０）。

【０１２３】以上のように、電子預金の口座の暗証番号のみならず、電子マネー自体にも使用者本人を認証するための機能を付与したので、防犯機能のさらなる向上が図られる。

【０１２４】次に、現金情報クリア処理を、図１７によって説明する。図１７に示すように、まず、ＬＳＩ－ＡのＣＰＵ２２が、図１６に示された光センサー２９からの出力信号に基づいて光センサー２９が光を検出したか否かを判定する（ステップ３２０）。

【０１２５】光センサー２９が光を検出しない場合（ステップ３２０否定判定）、そのまま待機し、通常の処理を続行する。光を検出した場合（ステップ３２０肯定判定）、ＣＰＵ２２がＲＡＭ２４に記録された現金情報等をクリアする（ステップ３２２）。すなわち、ＲＡＭ２４に記録されている現金情報、暗号コード及び暗号コード用のパラメータ等がクリアされる。

【０１２６】なお、光センサー２９が光を検出した場合には、予備電源１３からＬＳＩ－Ａへ電源が供給され、電子マネー１０へカードアクセス装置５２からの電源が供給されていない場合でも現金情報クリア処理が実行できるようになっている。

【０１２７】このように、ＬＳＩ－Ａの現金情報を引き出そうとする盗用者が、電子マネーを破壊しても、外部の光によって電子財布に記録された現金情報や暗号コード等がクリアされるので盗用を未然に防止することができる。

【０１２８】上記では、予備電源からＬＳＩ－Ａへ電源を供給する例について説明したが、受光可能なように光センサーをＬＳＩ－Ａに組み込むか、光センサーをＬＳＩ－Ａの近傍に配置し、受光したときに光センサーから出力される光電流を利用して、ＲＡＭに記録されている情報をクリアするようにしてもよい。なお、光電流が微弱な場合もあるが、ＲＡＭに記録されている情報をクリアする場合には、少なくとも暗号コードに関連する情報がクリアできればよい。

【０１２９】以上が、本発明に係る電子マネー１０の実施の形態であるが、上記例にのみ限定されるものではない。例えば、電子マネー１０は図２に示されたカードアクセス装置５２を介して外部機器３４と通信可能としたが、電子マネー１０に回線制御装置６０やモデム６２等を内蔵させて通信機能を備えたＩＣカードとして構成しても良い。

【０１３０】また、通信手段に関して公衆回線に限定されるものではなく、データ等を送受信できる他の通信網、例えばインターネット等を用いることもできる。

【０１３１】さらに、現金情報の入金、出金の処理は現金自動支払いシステムにのみ適用されるのではなく、情報現金の送受信が可能な装置、例えば自動販売機等にも適用可能である。この場合、ＬＳＩ－Ｂから出力されるコマンドも上記例に限られず、商品を売る側の口座への現金振込等、アプリケーションに応じて用意される。

【０１３２】また、残高チェックコマンドで検出された預金残高をディスプレイ６８に表示するようにしたが、ＬＳＩ－Ａが電子財布自体の残高を検出し、電気接点２１を介して当該残高を出力し、ディスプレイ６８に表示するようにしても良い。

【０１３３】また、図１７の現金情報クリア処理において、光が検出された場合だけではなく、電子マネー１０の図示しないケーシングが破壊された場合に、現金情報がクリアされるようにしても良い。

【０１３４】

【発明の効果】以上説明したように、請求項１～請求項１１の発明によれば、通信手段を介して遠隔にある現金の入金、出金等の処理を行うことができると共に、通信の盗聴による現金情報の盗用を有効に防止できる、という効果が得られる。

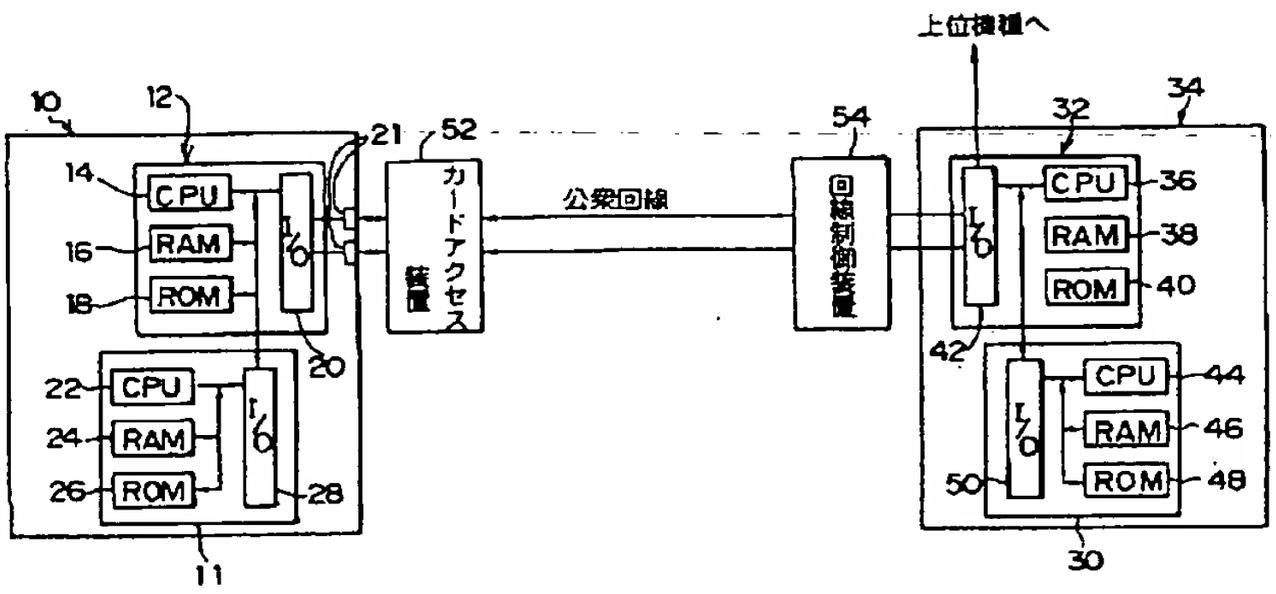
【図面の簡単な説明】

【図１】本発明の実施の形態に係る電子マネーの構成及び電子マネーと公衆回線を介して通信を行う外部機の構成を示す図である。

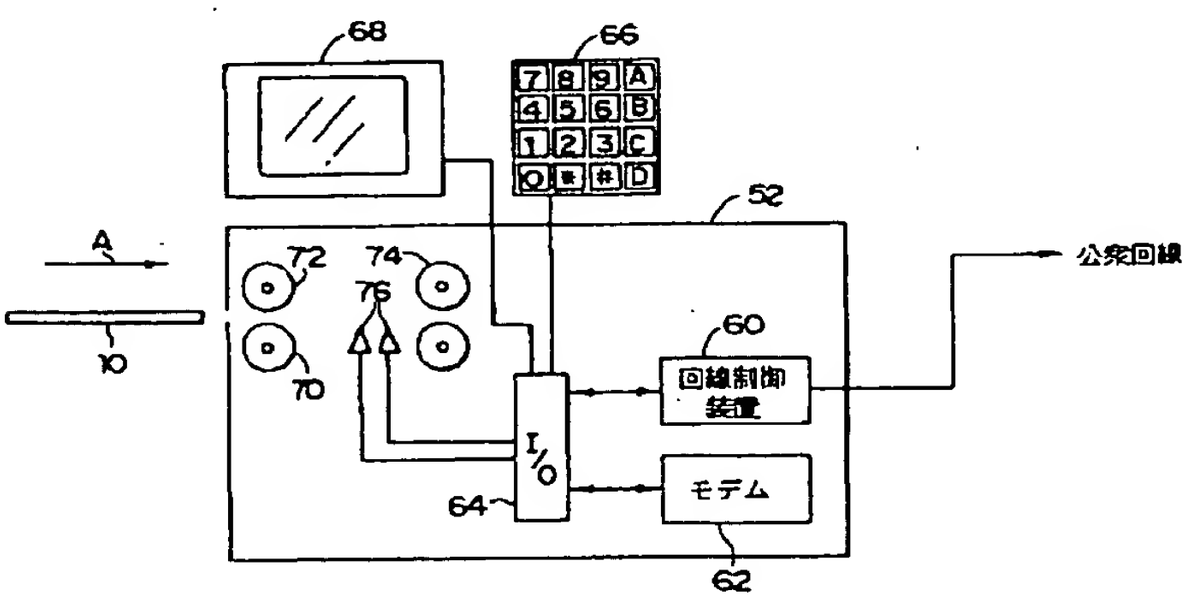
【図２】カードアクセス装置の構成を示す図である。

【図３】本実施の形態に係る通信処理の概要を示すフローチャートである。
【図４】本実施の形態に係るＬＳＩ－Ｂの通信処理を示すフローチャートである。
【図５】本実施の形態に係るＬＳＩ－Ｂ’の通信処理を示すフローチャートである。
【図６】本実施の形態に係るＬＳＩ－Ａの通信処理を示すフローチャートである。
【図７】本実施の形態に係るＬＳＩ－Ａ’の通信処理を示すフローチャートである。
【図８】有効期限設定処理の流れを示すフローチャートである。
【図９】アクセス禁止処理の流れを示すフローチャートである。
【図１０】使用頻度制限処理の流れを示すフローチャートである。
【図１１】アクセス可能先設定処理の流れを示すフローチャートである。
【図１２】認証機能の流れを示すフローチャートである。
【図１３】ＬＳＩ－Ｂが出力するコマンドのコードの構成を示す図である。
【図１４】登録された情報が記憶されているメモリ領域のデータ構成を示す図である。
【図１５】暗号化テーブルのデータ構成を示す図である。
【図１６】クロックを有するＬＳＩ－Ａの構成を示す図である。
【図１７】現金情報クリア処理の流れを示すフローチャートである。
【符号の説明】
１０　電子マネー
１１　ＬＳＩ－Ａ
１２　ＬＳＩ－Ｂ
３０　ＬＳＩ－Ａ’
３２　ＬＳＩ－Ｂ’
３４　外部機器

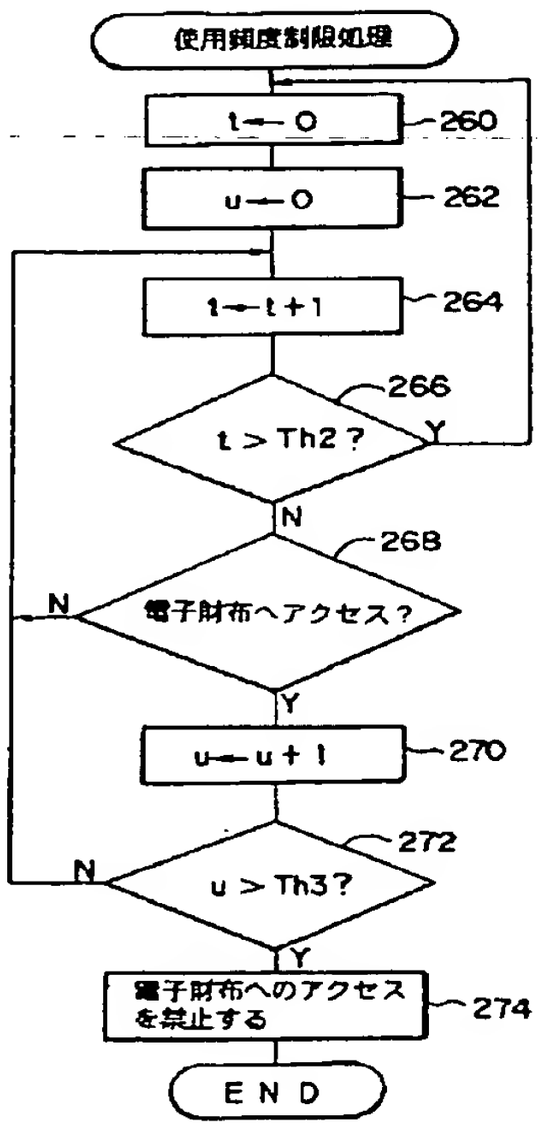
【図１】



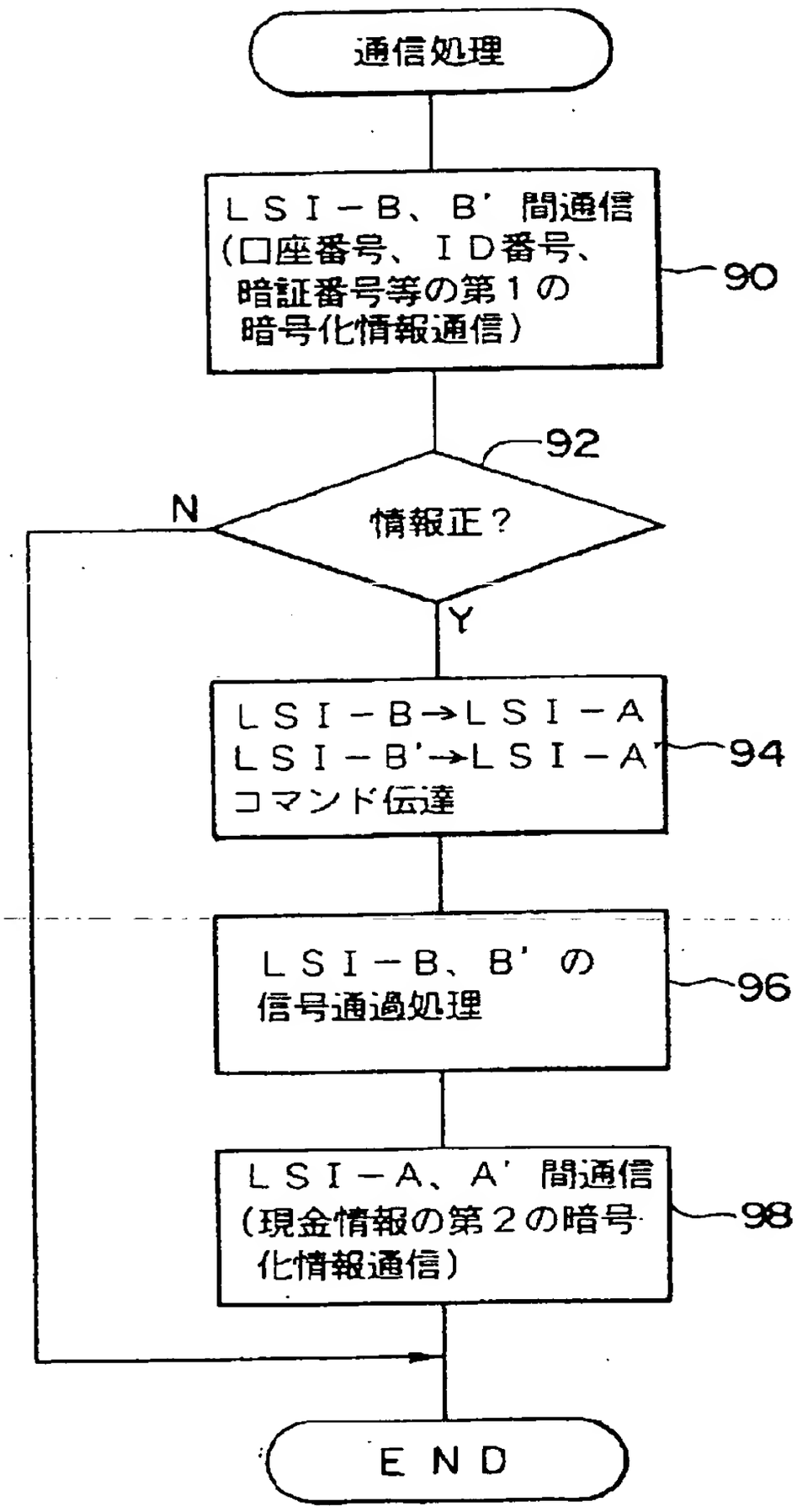
【図２】



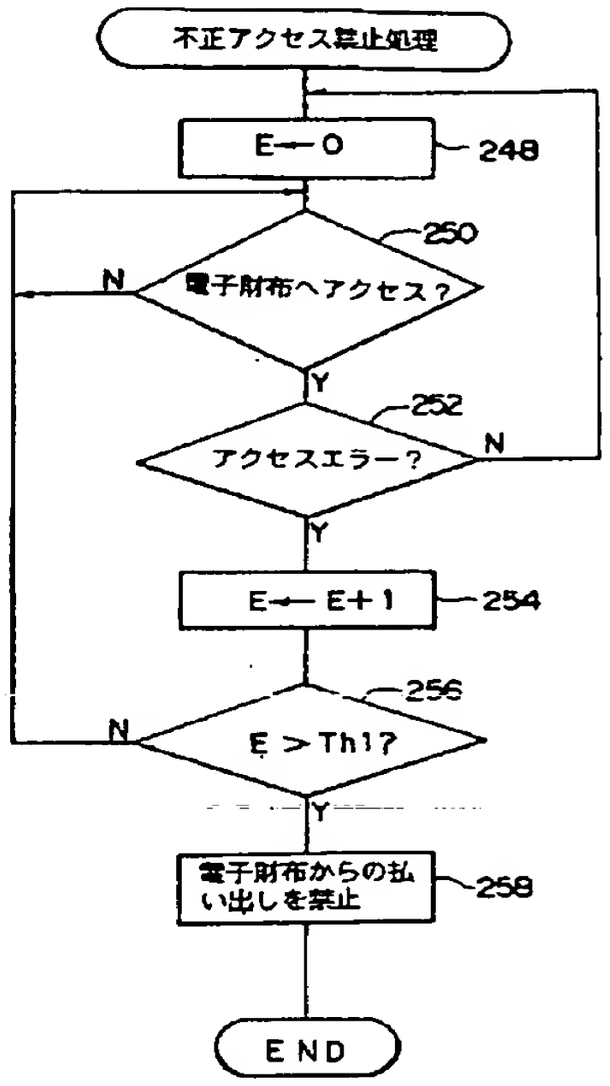
【図１０】



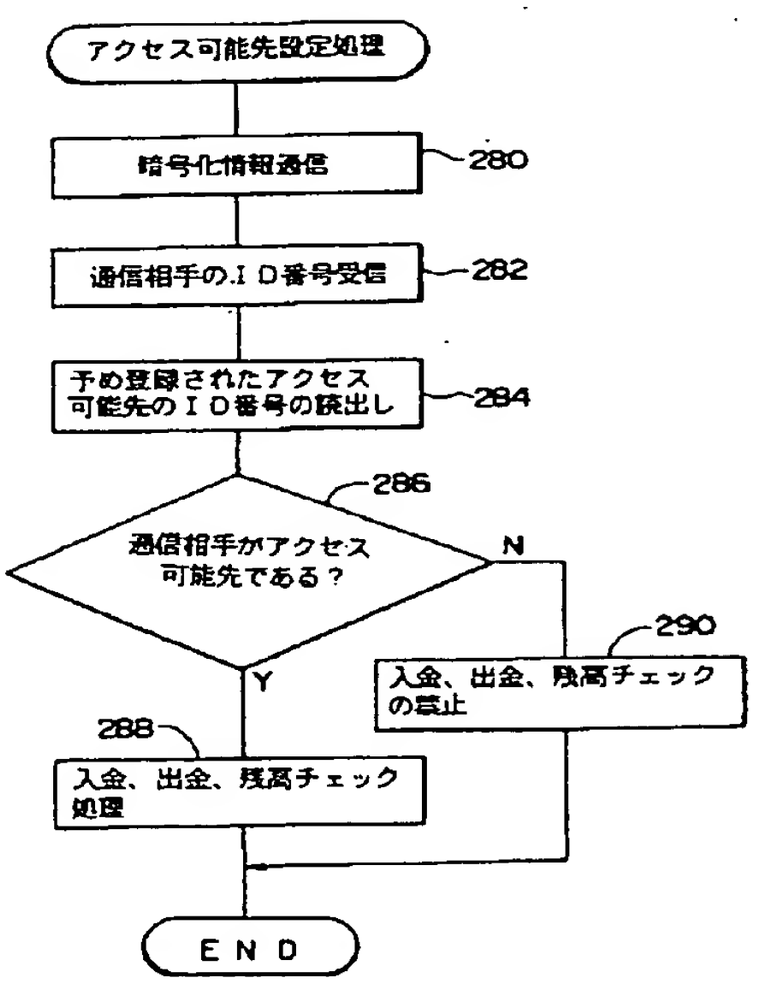
【図３】



【図９】



【図１１】

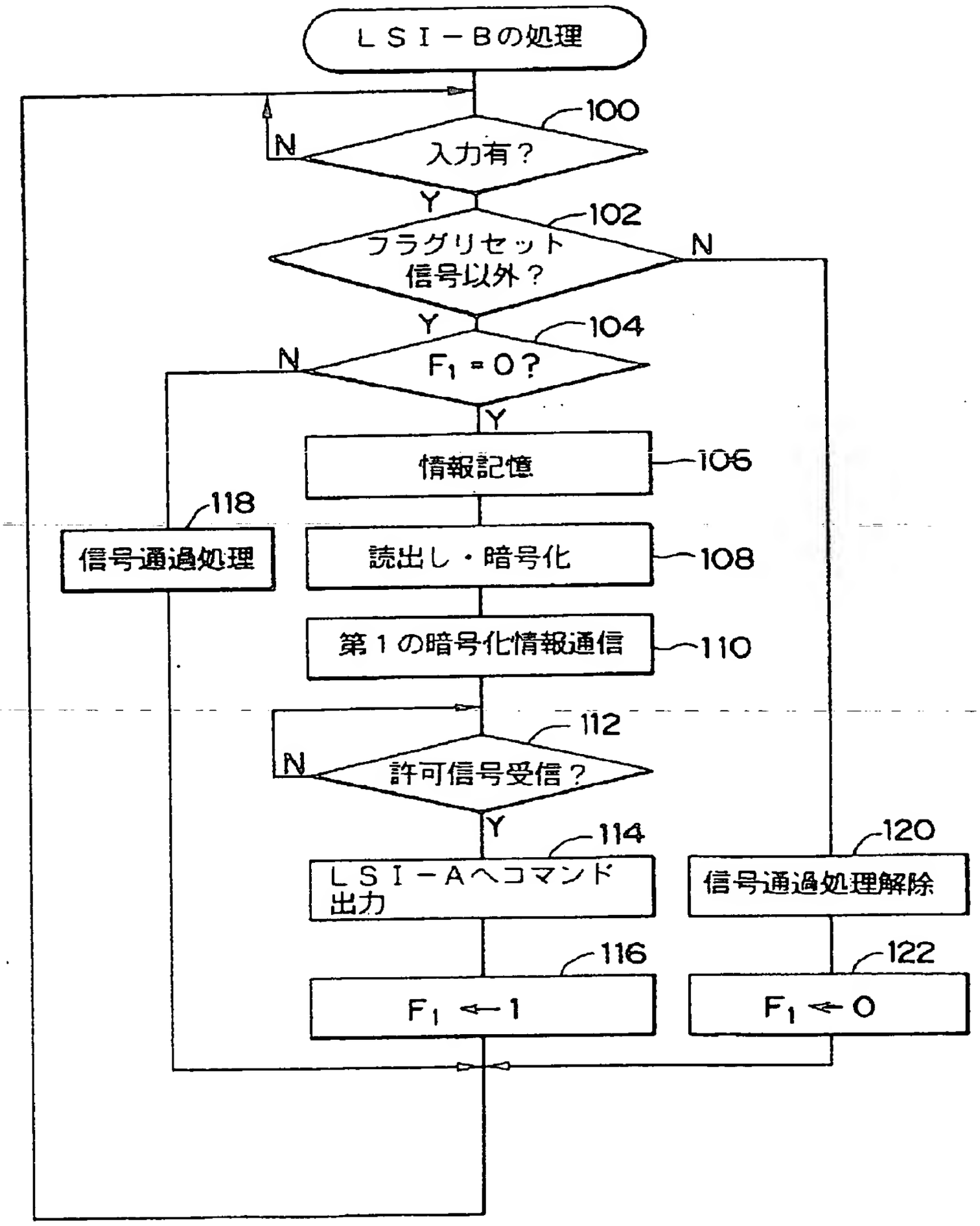


【図１５】

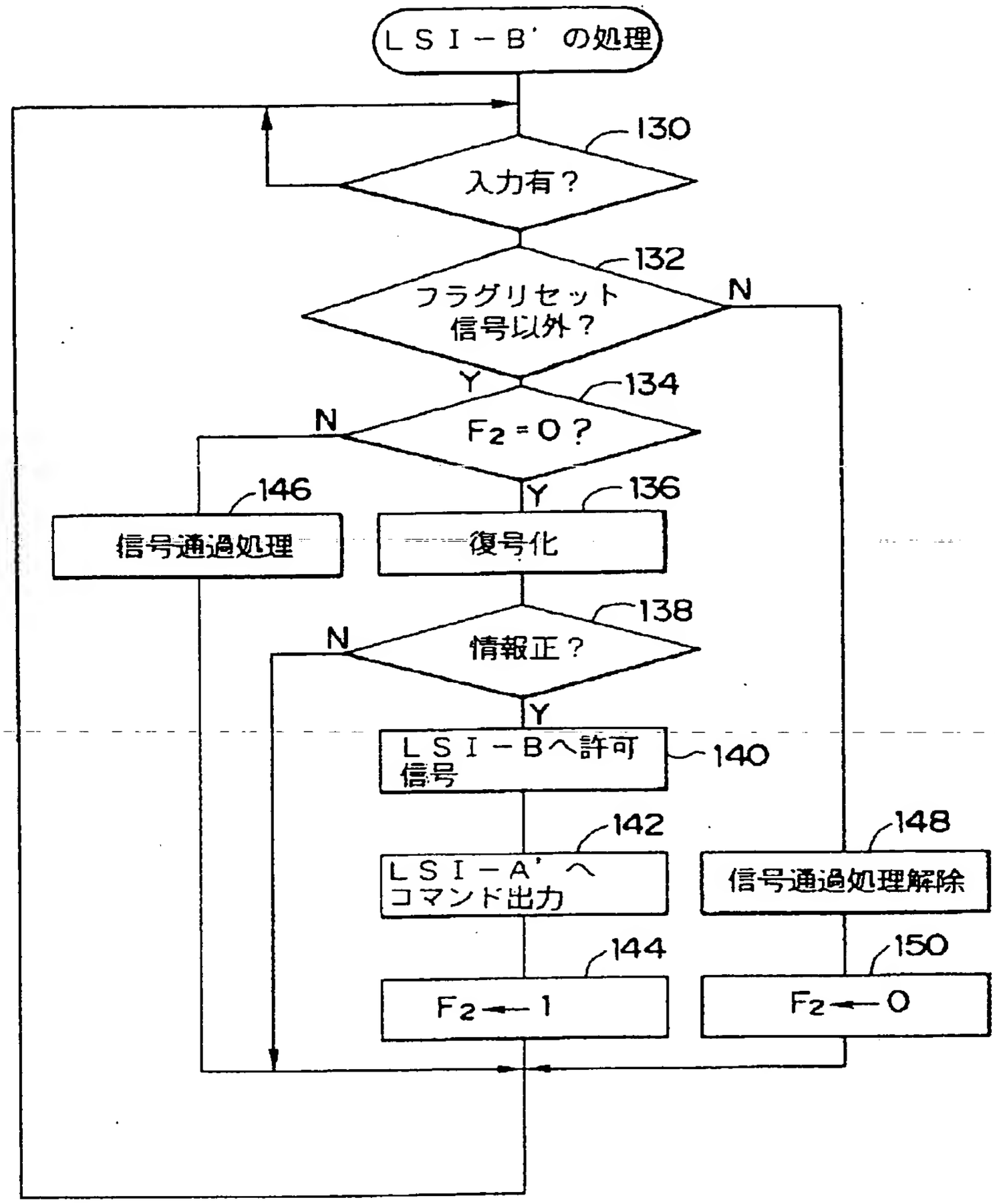
暗号化テーブル

番号	暗号化方法	暗号化コード
1	暗号化方法１	００００
2	暗号化方法２	０００１
3		
⋮	⋮	⋮

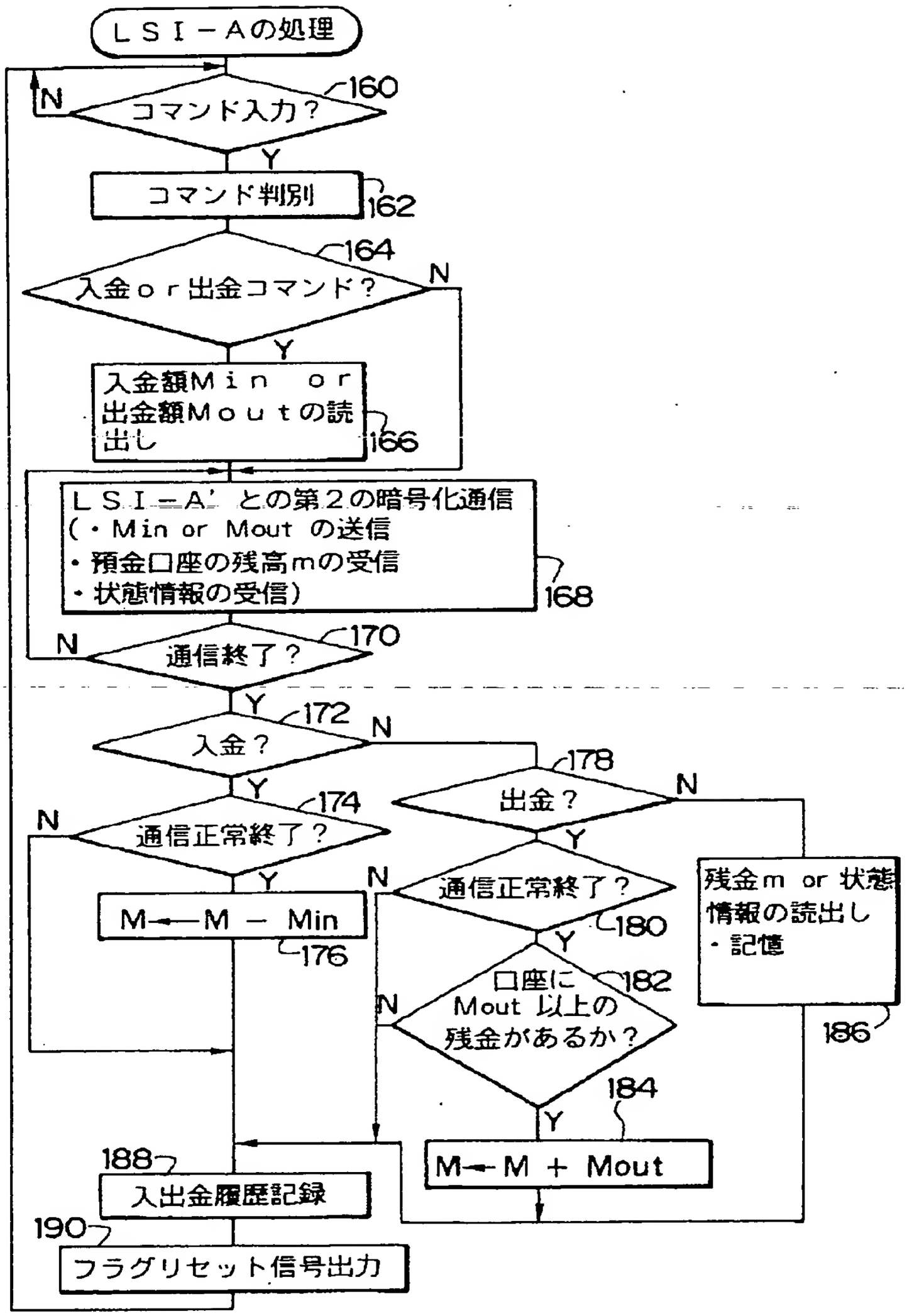
【図４】


ＬＳＩ－Ｂの処理
100
入力有？
N
Y
102
フラグリセット信号以外？
N
Y
104
F1＝0？
N
Y
106
情報記憶
108
読出し・暗号化
110
第１の暗号化情報通信
112
許可信号受信？
N
Y
114
ＬＳＩ－Ａへコマンド出力
116
F1 ←1
118
信号通過処理
120
信号通過処理解除
122
F1 ←0

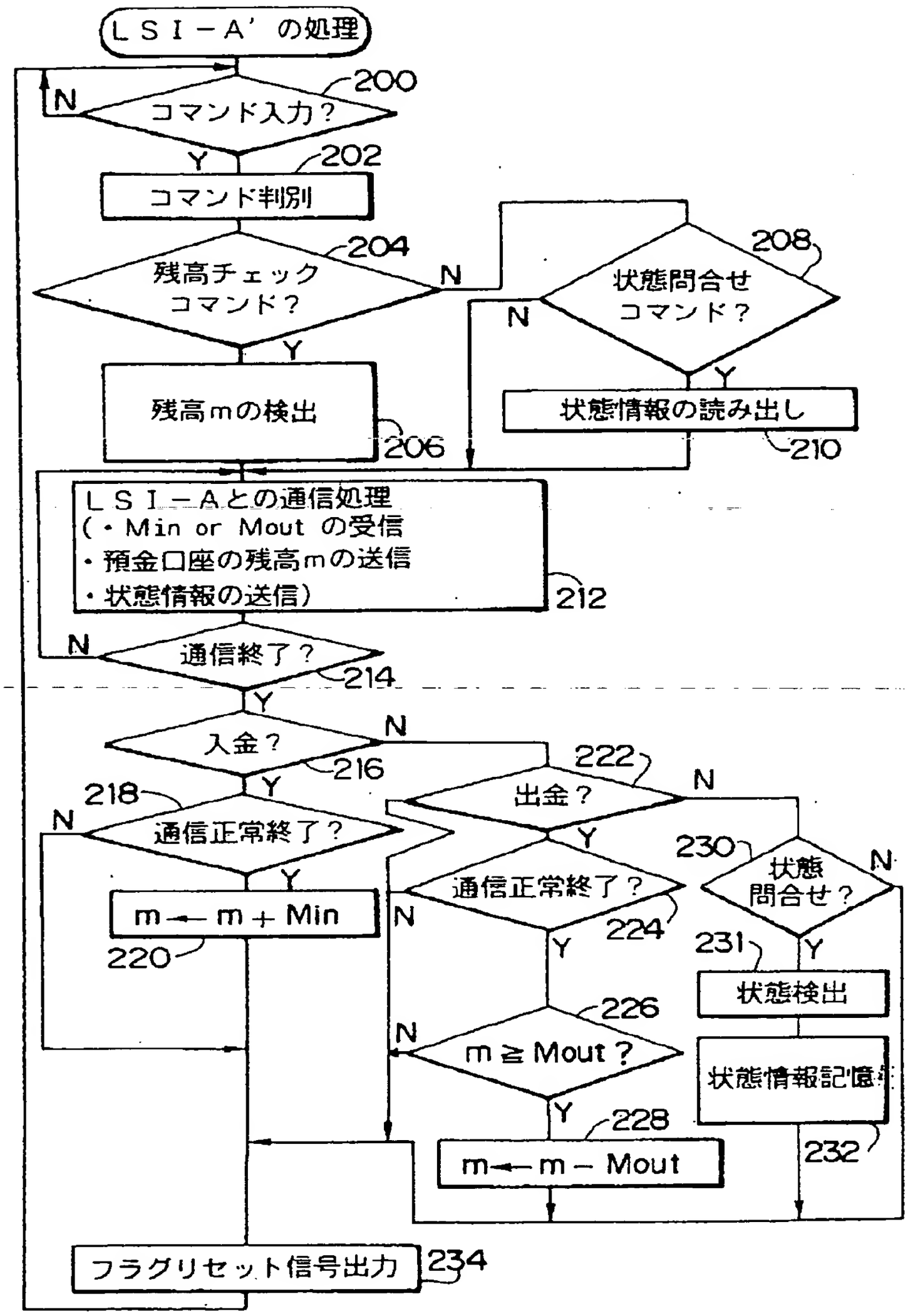
【図５】


ＬＳＩ－Ｂ' の処理
130
入力有？
132
フラグリセット
信号以外？
N
Y
134
F2＝0？
N
Y
146
信号通過処理
136
復号化
138
情報正？
N
Y
ＬＳＩ－Ｂへ許可
信号
140
142
ＬＳＩ－Ａ' へ
コマンド出力
144
F2←1
148
信号通過処理解除
150
F2←0

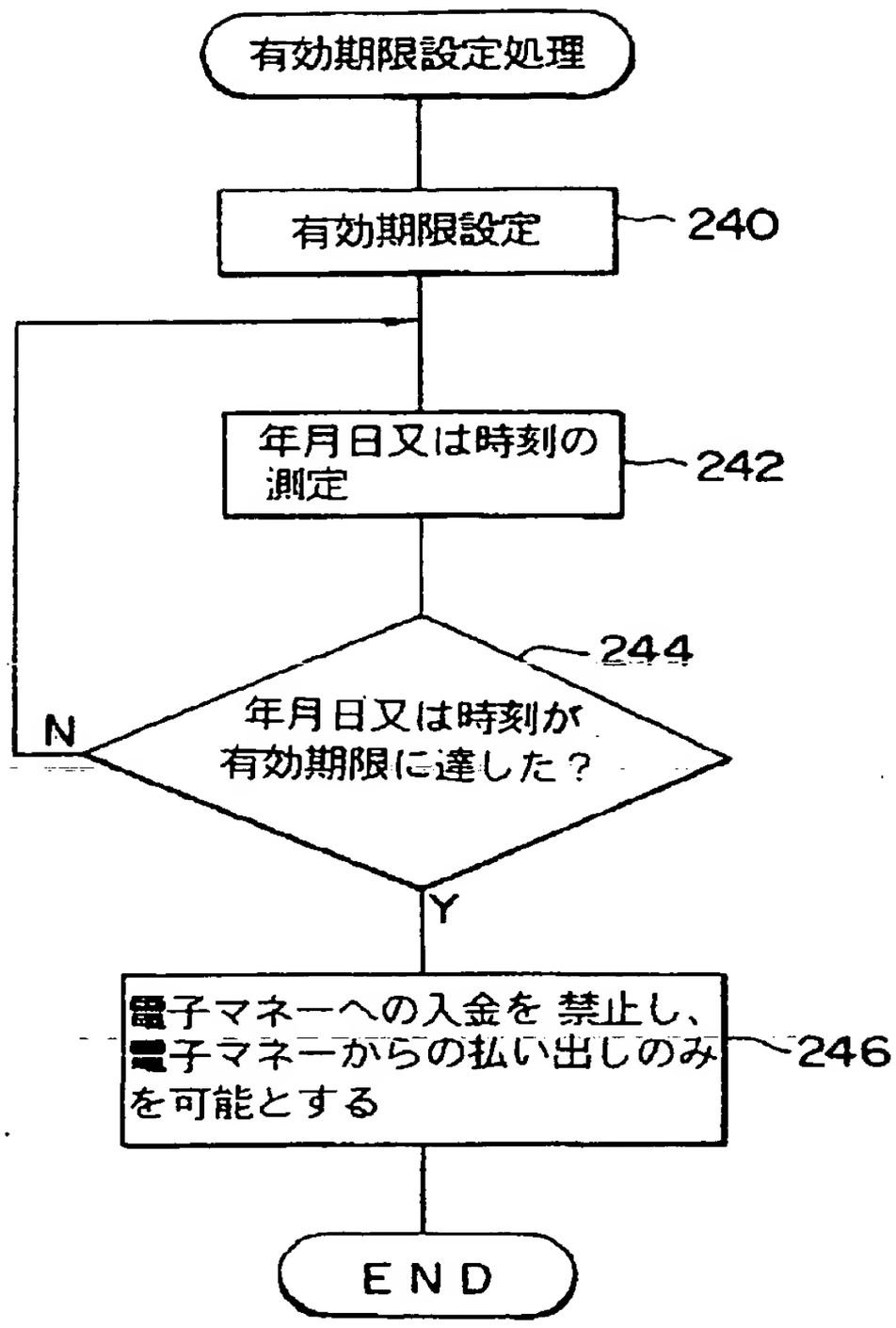
【図６】


ＬＳＩ－Ａの処理
160
N
コマンド入力？
Y
コマンド判別
162
164
入金ｏｒ出金コマンド？
N
Y
入金額Ｍｉｎ　ｏｒ
出金額Ｍｏｕｔの読
出し
166
ＬＳＩ－Ａ’との第２の暗号化通信
（・Ｍｉｎ or Ｍout の送信
・預金口座の残高ｍの受信
・状態情報の受信）
168
N
通信終了？
170
Y
172
入金？
N
Y
174
N
通信正常終了？
Y
M←M － Min
176
178
出金？
N
Y
N
通信正常終了？
180
Y
残金ｍ or 状態
情報の読出し
・記憶
186
口座に
Mout 以上の
残金があるか？
182
N
184
Y
M←M ＋ Mout
188
入出金履歴記録
190
フラグリセット信号出力

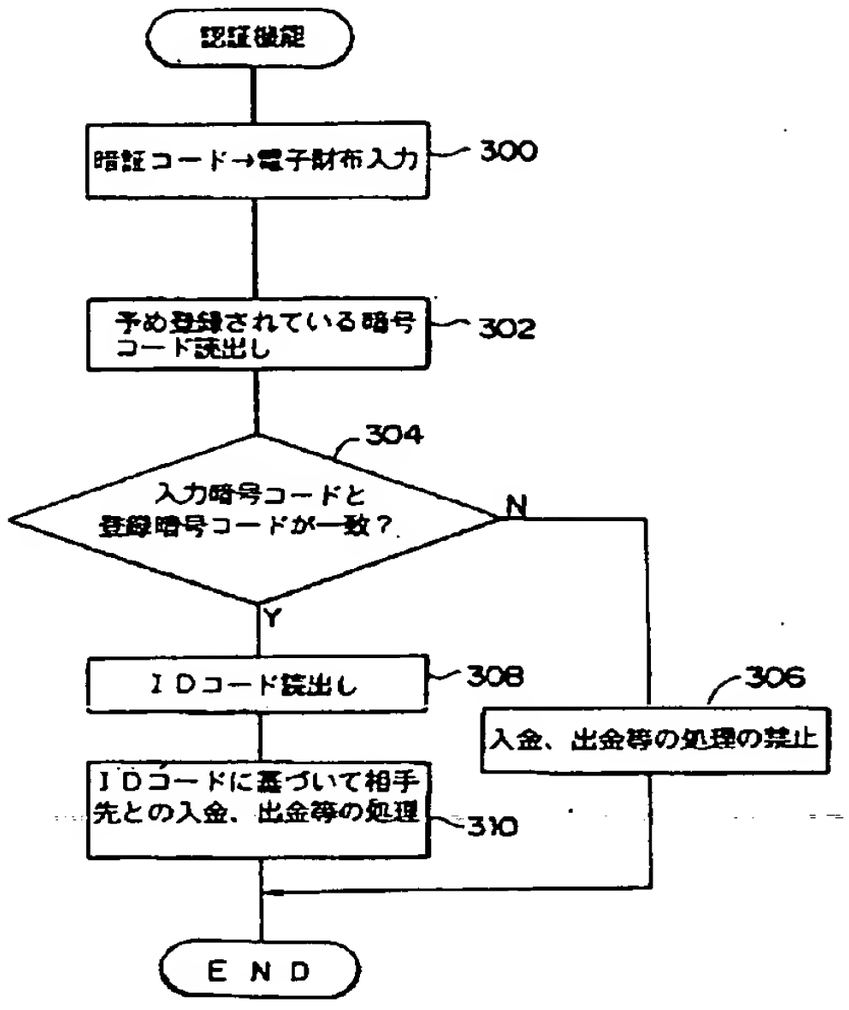
【図7】


LSI－A'の処理
200
N
コマンド入力？
Y
202
コマンド判別
204
残高チェック
コマンド？
N
Y
208
状態問合せ
コマンド？
N
Y
残高mの検出
206
状態情報の読み出し
210
LSI－Aとの通信処理
（・Min or Mout の受信
・預金口座の残高mの送信
・状態情報の送信）
212
N
通信終了？
214
Y
入金？
N
216
Y
218
N
通信正常終了？
Y
m ← m + Min
220
222
出金？
N
Y
通信正常終了？
224
N
Y
230
状態
問合せ？
N
Y
231
状態検出
226
N
m ≧ Mout ？
状態情報記憶
Y
228
m ← m － Mout
232
フラグリセット信号出力
234

【図８】



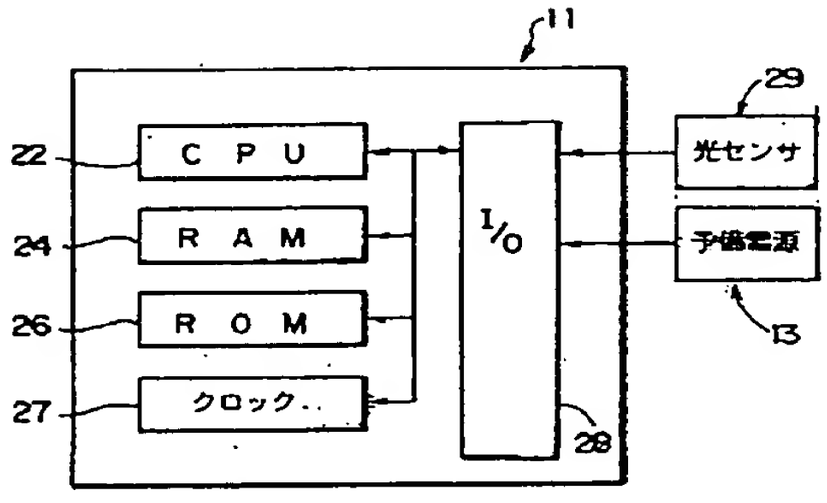
【図１２】



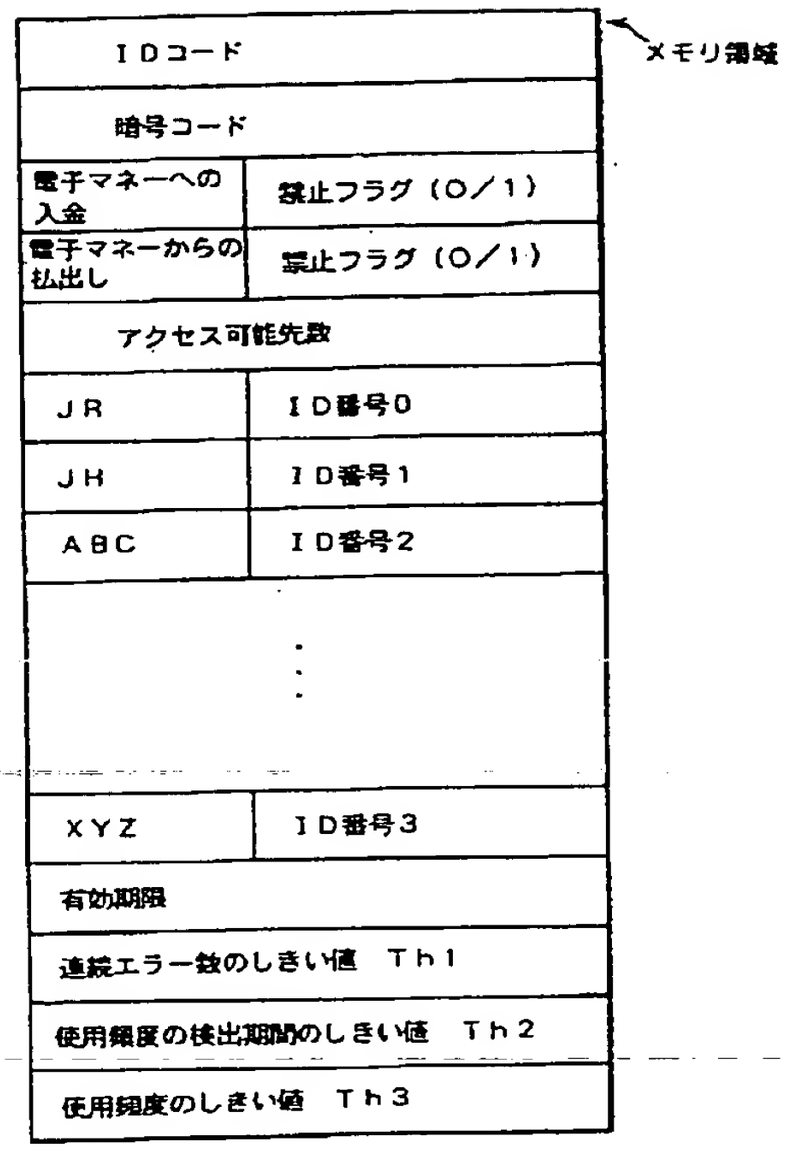
【図１３】

電子預金への入金コマンドコード	入金予定額Ｍｉｎ
電子預金への出金コマンドコード	出金予定額Ｍｏｕｔ
残高チェックコマンドコード	
状態問合せコマンドコード	状態の種類

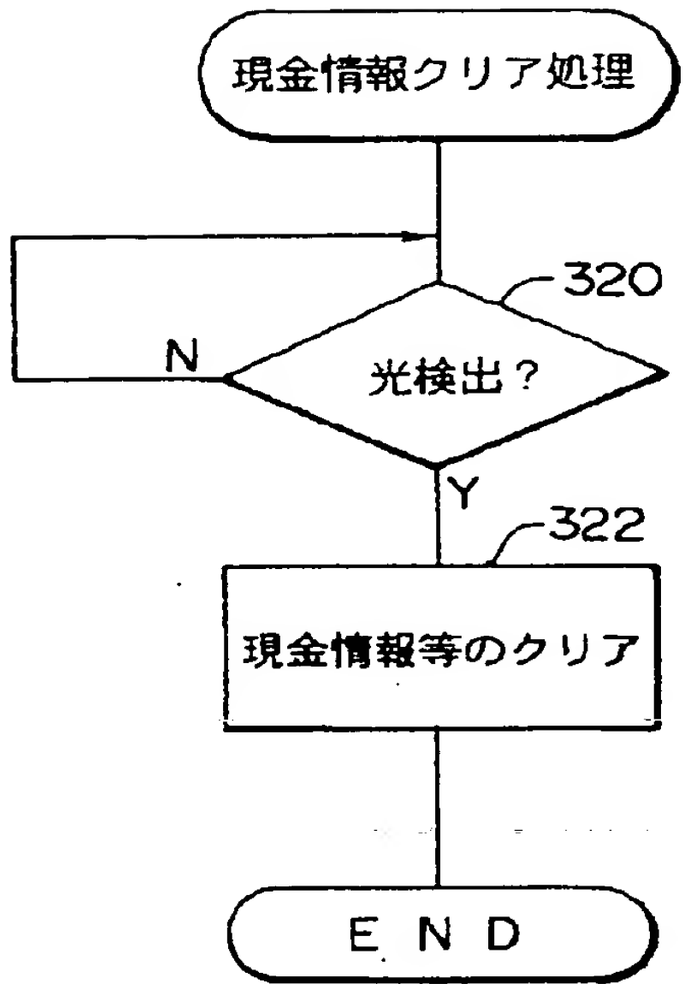
【図１６】



【図１４】


ＩＤコード
メモリ領域
暗号コード
電子マネーへの入金
禁止フラグ（０／１）
電子マネーからの払出し
禁止フラグ（０／１）
アクセス可能先数
ＪＲ
ＩＤ番号０
ＪＨ
ＩＤ番号１
ＡＢＣ
ＩＤ番号２
ＸＹＺ
ＩＤ番号３
有効期限
連続エラー数のしきい値　Ｔｈ１
使用頻度の検出期間のしきい値　Ｔｈ２
使用頻度のしきい値　Ｔｈ３

【図１７】


現金情報クリア処理
320
光検出？
N
Y
322
現金情報等のクリア
ＥＮＤ